

jfn

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Matthew Conover, Peter Szor
Assignee: Symantec Corporation
Title: RETURN-TO-LIBC ATTACK DETECTION USING BRANCH
TRACE RECORDS SYSTEM AND METHOD
Serial No.: 10/763,867 Filed: January 22, 2004
Examiner: Unknown Group Art 2131
Unit:
Docket No.: SYMC1044

Monterey, CA
May 18, 2004

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT
UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant(s) wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner.

U.S. PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	NAME
1)	5,822,517	10/13/1998	Dotan
2)	6,301,699	10/09/2001	Hollander et al.

OTHER DOCUMENTS

1)	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
2)	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: URL: http://www.windowsitlibrary.com/Content/356/06/2.html .
3)	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <URL: http://www.entercept.com/products/technology/kernelmode.asp >. No author provided.
4)	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <URL: http://www.entercept.com/products/technology/interception.asp >. No author provided.
5)	Gordon, J., "Understand ... the Stack (part 1)", pp. 1-8 [online]. Retrieved on August 27, 2003. Retrieved from the Internet:<URL: http://www.jorgon.freemove.co.uk/GoasmHelp/usstack1.htm >
6)	Chew, M. and Song, D., "Mitigating Buffer Overflows by Operating System Randomization", December 2002, 9 pages.
7)	"Entercept Continues to Dominate the Market in Buffer Overflow Protection", pg. 1-2 [online]. Retrieved on August 6, 2003. Retrieved from the Internet: <URL: http://www.entercept.com/news/uspr/07-09-02.asp >. No author provided.
8)	"IA-32 Intel® Architecture Software Developer's Manual; Volume 3: System Programming Guide", pgs. 15-11 to 15-22. 2002. No author provided.
9)	Dabak, P., Borate, M., Phadke, S., "Adding New System Services to the Windows NT Kernel", pp. 1-5 [online]. Retrieved December 16, 2003. Retrieved from the Internet: URL: http://www.windowsitlibrary.com/Content/356/07/1.html .
10)	Szor, U.S. Patent Application Serial No. 10/671,202, filed September 25, 2003, entitled "RETURN-TO-LIBC ATTACK BLOCKING SYSTEM AND METHOD".
11)	Szor, U.S. Patent Application Serial No. 10/360,341, filed February 6, 2003, entitled "SHELL CODE BLOCKING SYSTEM AND METHOD".
12)	Sobel et al., U.S. Patent Application Serial No. 10/140,149, filed May 6, 2002, entitled "ALTERATION OF MODULE LOAD LOCATIONS".

A PTO form 1449 listing these documents is enclosed.

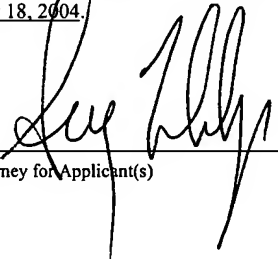
Citation of the above documents shall not be construed as:

1. an admission that the documents are necessarily prior art with respect to the instant invention;
2. a representation that a search has been made, other than as described above; or
3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

The Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

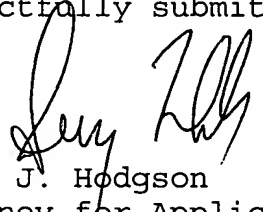
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 18, 2004.



Attorney for Applicant(s)

May 18, 2004
Date of Signature

Respectfully submitted,


Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
(831) 655-0880

Form PTO-1449

Atty Docket No.

Serial No.

SYMC1044

10/763,867

INFORMATION DISCLOSURE CITATION

IN AN APPLICATION

Applicant(s)

Matthew Conover et al.

Filing Date

January 22, 2004

Group

2131

(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA	5,822,517	10/13/1998	Dotan	395	186	
	AB	6,301,699	10/09/2001	Hollander et al.	717	4	
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

AR	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
AS	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: URL:http://www.windowsitlibrary.com/Content/356/06/2.html .
AT	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: < URL:http://www.entercept.com/products/technology/kernelmode.asp >. No author provided.

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449				Atty Docket No. SYMC1044		Serial No. 10/763,867	
INFORMATION DISCLOSURE CITATION IN AN APPLICATION				Applicant(s) Matthew Conover et al.			
(Use several sheets if necessary)				Filing Date January 22, 2004		Group 2131	

U.S. PATENT DOCUMENTS							
EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS								
							Translation	
DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO		
AL								
AM								
AN								
AO								
AP								

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
AR	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <URL:http://www.entercept.com/products/technology/interception.asp>. No author provided.
AS	Gordon, J., "Understand ... the Stack (part 1)", pp. 1-8 [online]. Retrieved on August 27, 2003. Retrieved from the Internet: <URL:http://www.jorgon.freemove.co.uk/GoasmHelp/usstack1.htm>
AT	Chew, M. and Song, D., "Mitigating Buffer Overflows by Operating System Randomization", December 2002, 9 pages.

Examiner	Date Considered
----------	-----------------

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449				Atty Docket No. SYMC1044		Serial No. 10/763,867	
INFORMATION DISCLOSURE CITATION IN AN APPLICATION				Applicant(s) Matthew Conover et al.			
(Use several sheets if necessary)				Filing Date January 22, 2004		Group 2131	

U.S. PATENT DOCUMENTS							
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AF						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS								
							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

OTHER DOCUMENTS		(Including Author, Title, Date, Pertinent Pages, Etc.)
	AR	"Entercept Continues to Dominate the Market in Buffer Overflow Protection", pg. 1-2 [online]. Retrieved on August 6, 2003. Retrieved from the Internet: <URL:http://www.entercept.com/news/uspr/07-09-02.asp>. No author provided.
	AS	"IA-32 Intel® Architecture Software Developer's Manual; Volume 3: System Programming Guide", pgs. 15-11 to 15-22. 2002. No author provided.
	AT	Dabak, P., Borate, M., Phadke, S., Adding New System Services to the Windows NT Kernel", pp. 1-5 [online]. Retrieved December 16, 2003. Retrieved from the Internet: URL:http://www.windowsitlibrary.com/Content/356/07/1.html.

Examiner	Date Considered
----------	-----------------

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449				Atty Docket No. SYMC1044		Serial No. 10/763,867	
INFORMATION DISCLOSURE CITATION IN AN APPLICATION				Applicant(s) Matthew Conover et al.			
(Use several sheets if necessary)				Filing Date January 22, 2004		Group 2131	

U.S. PATENT DOCUMENTS							
EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

FOREIGN PATENT DOCUMENTS								
							Translation	
DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO		
AL								
AM								
AN								
AO								
AP								

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
AR	Szor, U.S. Patent Application Serial No. 10/671,202, filed September 25, 2003, entitled "RETURN-TO-LIBC ATTACK BLOCKING SYSTEM AND METHOD".
AS	Szor, U.S. Patent Application Serial No. 10/360,341, filed February 6, 2003, entitled "SHELL CODE BLOCKING SYSTEM AND METHOD".
AT	Sobel et al., U.S. Patent Application Serial No. 10/140,149, filed May 6, 2002, entitled "ALTERATION OF MODULE LOAD LOCATIONS".

Examiner	Date Considered
----------	-----------------

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).